

# **ANALYSIS OF INTRUSION DETECTION SYSTEM (IDS) IN BORDER GATEWAY PROTOCOL**

**By Muhammad Mujtaba**

**Principal Supervisor: Dr.Priyadarsi Nanda**

**Co- Supervisor: Prof. Xiangjian He**



**FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY  
UNIVERSITY OF TECHNOLOGY, SYDNEY  
2012.**

*“Elevate yourself so high that even God, before issuing every decree of destiny, should ask you: Tell me, what is your intent?” – Dr. Allama Iqbal*

*Dedicated to*  
*my mom, Mrs.Saira*

## **CERTIFICATE OF AUTHORSHIP/ORIGINALITY**

I certify that the work in this thesis has not previously been submitted for a degree nor has it been submitted as part of requirements for a degree except as fully acknowledged within the text.

I also certify that the thesis has been written by me. Any help that I have received in my research work and the preparation of the thesis itself has been acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

Signature of Candidate

---

## **ACKNOWLEDGMENTS**

It is a pleasure to thank the many people who made this thesis possible.

It is difficult to overstate my gratitude to my Ph.D. supervisor, Dr. Priyadarsi Nanda. With his enthusiasm, his vast experience and knowledge, and his great efforts to explain things clearly and simply, he helped reduce the complexity of this thesis and made it simple for me. Throughout my thesis-writing period, he provided encouragement, sound advice, good teaching, good company, and lots of good ideas.

I would like to thank Professor Xiangjian He for all the help and support he provided me in the areas of pattern recognition and network security; I would like to extend my sincere thanks to all my research fellow students for their contribution, feedback and for arranging weekly meetings for the exchange of cutting edge ideas which in all helped me with this research.

I wish to thank my good friends (Esha Dutt) - for proof reading and paper editing, Hamid Ghous (PhD candidate) for helping me with writing the computer program, getting through the difficult times and for all the emotional support, entertainment, and caring they provided.

I wish to thank my entire family for providing me with emotional and loving support. Lastly, and most importantly, I wish to thank my mum, Mrs. Saira, who raised me, supported me, taught me, and loved me. To whom I dedicate this thesis.

## ABSTRACT

Border Gateway Protocol (BGP) is the de-facto inter-domain routing protocol used across thousands of Autonomous Systems (AS) joined together in the Internet. The main purpose of BGP is to keep routing information up-to-date across the Autonomous System (AS) and provide a loop free path to the destination. Internet connectivity plays a vital role in organizations such as in businesses, universities and government organisations for exchanging information. This type of information is exchanged over the Internet in the form of packets, which contain the source and destination addresses. Because the Internet is a dynamic and sensitive system which changes continuously, it is therefore necessary to protect the system from intruders. Security has been a major issue for BGP. Nevertheless, BGP suffers from serious threats even today, DoS attack is the major security threat to the Internet today, among which, is the TCP SYN flooding, the most common type of attack. The aim of this DoS attack is to consume large amounts of bandwidth. Any system connected to the Internet and using TCP services are prone to such attacks. It is important to detect such malicious activities in a network, which could otherwise cause problems for the availability of services.

This thesis proposes and implements two new security methods for the protection of BGP data plane, *“Analysis of BGP Security Vulnerabilities”* and *“Border Gateway Protocol Anomaly Detection using Failure Quality Control Method”* to detect the malicious packets and the anomaly packets in the network.

The aim of this work is to combine the algorithms with the Network Data Mining (NDM) method to detect the malicious packets in the BGP network. Furthermore, these patterns can be used in the database as a signature to capture the incidents in the future.

## TABLE OF CONTENTS

<b>CHAPTER 1 INTRODUCTION .....</b>	<b>16</b>
1.1.    MOTIVATION AND OBJECTIVE .....	17
A. <i>Network Data Analysis</i> .....	18
B. <i>Classification</i> .....	18
1.2.    THESIS STRUCTURE .....	19
1.3.    PUBLICATION .....	19
<b>CHAPTER 2 LITERATURE REVIEW .....</b>	<b>20</b>
<b>CHAPTER 3 BORDER GATEWAY PROTOCOL .....</b>	<b>26</b>
BGP MESSAGE TYPES .....	26
BGP ROUTING ATTRIBUTES & ROUTING POLICY .....	28
IP ADDRESS & AS NUMBERS ALLOCATOR .....	30
SUMMARY .....	<b>32</b>
<b>CHAPTER 4 BGP SECURITY THREATS &amp; COUNTER MEASURES .....</b>	<b>35</b>
TYPES OF ATTACKS ON BGP .....	35
4.1.1    Spoofing .....	36
4.1.2    Session Hijacking .....	38
4.1.3    Route Flapping .....	39
4.1.4    Route De-aggregation .....	40
4.1.5    Unallocated Route Injection .....	40
4.1.6    Denial of Service (DoS) .....	40
4.1.7    Misconfiguration .....	41
BGP SECURITY COUNTERMEASURES .....	42
A.    PROTECTING THE ONGOING BGP SESSION BETWEEN ROUTERS .....	42
B.    CRYPTOGRAPHY METHOD .....	45
C.    ROUTE FILTERING .....	47
D.    PHYSICAL SECURITY .....	48

SUMMARY .....	48
<b>CHAPTER 5 FIREWALL &amp; INTRUSION DETECTION SYSTEM .....</b>	<b>50</b>
INTRODUCTION TO INTRUSION DETECTION SYSTEM.....	52
TYPES OF INTRUSION DETECTION .....	53
COMPONENTS OF IDS.....	54
IDS ARCHITECTURE .....	56
IDS CHALLENGES.....	58
ACCESS CAPABILITIES.....	59
SUMMARY .....	64
<b>CHAPTER 6 RESEARCH METHODOLOGY &amp; EXPERIMENTATION.....</b>	<b>66</b>
RESEARCH MODEL.....	66
DATA EXTRACTION FROM KDD CUP 99.....	67
EXPERIMENTAL ANALYSIS .....	69
<b>EXPERIMENT 1.....</b>	<b>69</b>
A. CUSUM (CUMULATIVE SUM) ALGORITHM .....	69
B. ADAPTIVE THRESHOLD ALGORITHM.....	70
C. K-MEAN CLUSTER ALGORITHM .....	72
1) HIGH INTENSITY ATTACKS .....	73
2) LOW INTENSITY ATTACKS.....	74
3) FALSE ALARM & DETECTION PROBABILITY. ....	77
PERFORMANCE ANALYSIS .....	77
<b>EXPERIMENT 2.....</b>	<b>78</b>
1) HIGH INTENSITY ATTACKS .....	79
2) LOW INTENSITY ATTACKS.....	80
3) DETECTION PROBABILITY VS FALSE ALARM.....	81
<b>CHAPTER 7 FUTURE WORK AND CONCLUSION .....</b>	<b>85</b>
7.1 CONTRIBUTION OF THESIS .....	85

7.2 FUTURE WORK.....	86
7.3 CONCLUSION .....	87
REFERENCES .....	90



## LIST OF FIGURES

Figure 3-1: IP address and AS delegation from the root (IANA) .....	31
Figure 3-2: An AS advertises its number to neighbour .....	32
Figure 4-1: Port attack .....	37
Figure 4-2: IP address attack .....	37
Figure 4-3: False route injection .....	37
Figure 4-4: TCP Sequencing .....	38
Figure 4-5: Packet Time to Live (TTL) technique .....	38
Figure 4-6: Router C causing Session Hijacking .....	39
Figure 4-7: Router C causing Route Flapping .....	39
Figure 4-8: Denial of Service Attacks caused by Router C .....	41
Figure 4-9: Encrypting Session between the session .....	42
Figure 4-10: Encrypting message between the session .....	43
Figure 4-11 : Encrypting UPDATE message between the session Encrypting message between the session .....	43
Figure 4-12: Generalized TTL technique .....	44
Figure 4-13: IPSec Tunneling .....	45
Figure 4-14: Revoking Digital Certificate from the Root Level .....	47
Figure 4-15: Filtering Malicious Route .....	48
Figure 5-1: IDS Components .....	55
Figure 5-2: In-Line Mode .....	56
Figure 5-3: Switched Port Analyser Mode .....	57
Figure 5-4: Passive Mode .....	57
Figure 5-5: Tap mode .....	58
Figure 5-6: IDPS Management Cycle .....	64
Figure 6-1: KDD Process Model .....	67
Figure 6-2: Before Clustering .....	73
Figure 6-3: After clustering .....	73
Figure 6-5: HI-Adaptive threshold .....	74

Figure 6-6:HI- K mean .....	74
Figure 6-4: HI- CUSUM .....	74
Figure 6-8:LI-Adaptive threshold .....	75
Figure 6-9:LI- K means.....	75
Figure 6-7: LI CUSUM .....	75
Figure 6-10:CUSUM high intensity attack.....	76
Figure 6-11:CUSUM low intensity attack.....	76
Figure 6-12:Adaptive threshold high intensity attack .....	76
Figure 6-13:Adaptive threshold low intensity attack .....	76
Figure 6-14:K mean high intensity attack .....	76
Figure 6-15:K mean low intensity attack .....	76
Figure 6-16: Control chart.....	79
Figure 6-17: High intensity attacks .....	80
Figure 6-18: Low intensity attacks .....	81
Figure 6-19: Receiver Operator Curve (ROC) for High Intensity Attack .....	83
Figure 6-20: Receiver Operator Curve (ROC) for Low Intensity Attack .....	83

## LIST OF TABLES

Table 3-1: OPEN Message Length .....	27
Table 3-2: UPDATE Message Length .....	27
Table 3-3: NOTIFICATION Message Length.....	27
Table 3-4: KEEPALIVE Message Length .....	28
Table 6-1:KDD Extracted Dataset.....	68
Table 6-2: Receiver Operator Curve (ROC) data for High Intensity Attack.....	82
Table 6-3: Receiver Operator Curve (ROC) data for Low Intensity Attack .....	82

## LIST OF ACRONYMS

<b>ACL</b>	Access Control List
<b>AH</b>	Authentication Header
<b>AR</b>	Alarm Rate
<b>AS</b>	Autonomous System
<b>ASN</b>	Autonomous System Number
<b>BCP</b>	Best Common Practices
<b>BGP</b>	Border Gateway Protocol
<b>CPU</b>	Central Processing Unit
<b>CSI</b>	Computer Security Institute
<b>CUSUM</b>	Cumulative Sum
<b>DDoS</b>	Distributed Denial of Service
<b>DoS</b>	Denial of Service
<b>DR</b>	Detection Rate
<b>EBGP</b>	Exterior BGP
<b>ESP</b>	Encapsulating Security Payload
<b>EWMA</b>	Exponentially Weight Moving Average
<b>FCE</b>	Flow Connection Entropy
<b>FP</b>	False Positive
<b>FQC</b>	Failure Quality Control
<b>FTP</b>	File Transfer Protocol
<b>GTSM</b>	Generalized TTL Security Mechanism
<b>HIDS</b>	Host Intrusion Detection Sensor

<b>HHH</b>	Hierarchical Heavy Hitter
<b>HTTP</b>	Hyper Text Transfer Protocol
<b>HTTPS</b>	Hyper Text Transfer Protocol Secure
<b>IANA</b>	Internet Assigned Number Authority
<b>IBGP</b>	Interior BGP
<b>IDS</b>	Intrusion Detection System
<b>IDSC</b>	Intrusion Detection Systems Consortium
<b>IPS</b>	Intrusion Prevention System
<b>IPSec</b>	Internet Protocol Security
<b>IRR</b>	Internet Routing Registers
<b>IRV</b>	Internet Routing Validation
<b>ISP</b>	Internet Service Provider
<b>KDD</b>	Knowledge Discovery and Data
<b>LCL</b>	Lower Control Limit
<b>MAC</b>	Message Authentication Code
<b>MD</b>	Message Digestion
<b>MED</b>	Multi-Exit Discriminator
<b>MTU</b>	Maximum Transmission Unit
<b>NADA</b>	Network Anomaly Detection Algorithm
<b>NDM</b>	Network Data Mining
<b>NIDS</b>	Network Intrusion Detection Sensor
<b>NTM</b>	Network Traffic Management
<b>OS</b>	Operating System
<b>PCA</b>	Principal Component Analysis

<b>PTA</b>	Pakistan Telecommunication Authority
<b>PGBGP</b>	Pretty Good BGP
<b>QoS</b>	Quality of Service
<b>RIR</b>	Regional Internet Registries
<b>ROC</b>	Receiver Operator Curve
<b>RST</b>	Rough Set Theory
<b>S-BGP</b>	Secured-BGP
<b>SDM</b>	Security Device Manager
<b>SHA</b>	Standard Hashing Algorithm
<b>SIM</b>	Source IP Monitoring
<b>SLA</b>	Service Level Agreement
<b>SoBGP</b>	Secure Origin BGP
<b>SPAN</b>	Switched Port Analyser
<b>SVM</b>	Support Vector Machine
<b>TCP</b>	Transport Communication Protocol
<b>ToS</b>	Term of Service
<b>TP</b>	True Positive
<b>TTL</b>	Time to Live
<b>UCL</b>	Upper Control Limit
<b>UDP</b>	User Datagram Protocol
<b>UPS</b>	Uninterruptible Power Supply
<b>URCA</b>	Unsupervised Root Cause Analysis
<b>VPN</b>	Virtual Private Network
<b>WGLR</b>	Wavelet Generalized Likelihood Ratio

